

Privacy Compliance 101

Privacy audits can feel overwhelming. This guide will help you feel more confident as you prepare for your next privacy audit.



Privacy audits are hard.

We believe if you're going to do an audit, it should be worth it.

We know that when it comes to privacy, you want to understand and comply with privacy requirements so you can keep doing business with your clients and use your privacy program as a strategic advantage to gain new clients. In order to do that, you need a quality privacy audit process that gives you results you can trust and that ensures you respect data privacy. The problem is, privacy laws and regulations are constantly changing, and the process feels overwhelming.

We hope this guide makes your privacy audit less complicated and a little easier to get started.



Table of Contents

3	An Introduction to Privacy
4	What You need to Know Before Your Privacy Audit
5	How a Privacy Audit Benefits Your Organization
6	How the Privacy Audit Process Works
8	Major Data Privacy Laws and Regulations
11	Partner with KirkpatrickPrice

An Introduction to Privacy

Privacy laws and regulations have been an ongoing initiative in the US since 1974. And since then, new and broader privacy laws and standards are popping up around the world frequently. At the same time, organizations possess more personal data than ever before, and a lot of that data is required by law to be protected in one way or another.

Since the introduction of Europe's General Data Protection Regulation (GDPR) in 2016, privacy awareness has grown through online privacy notices, cookie pop-ups, business to business privacy compliance expectations, and highly publicized fines for noncompliance. Even more, data privacy is considered a right that belongs to individuals even when those individuals share their data with organizations. Fortunately, our privacy audits affirm your organization's compliance with regulatory requirements like:



GDPR



CCPA



SOC 2 Privacy



HIPAA

A privacy audit will also focus on the privacy obligations that appear in organization's B2B contracts, B2C privacy notices, cookie pop ups, and more, so you can make sure all of your bases are covered when it comes to privacy compliance.

What You Need to Know Before Your Privacy Audit

When it comes to preparing for your privacy audit, you need to understand what types of personal data your organization possesses, why you process that personal data, how it's stored, who it's shared with, and what you're doing to keep it safe. Understanding how your organization truly processes the personal data you receive is an important step to complying with the privacy requirements that have been set in place.

Establishing an effective internal privacy framework is a great way to prepare for a privacy audit because the framework will give your organization a chance to build a principle-based, rather than a process-based, privacy program. All data privacy laws, contracts, and industry standards are built on the same privacy principles, some of which are listed in the bullets below. Creating a privacy program based on these principles, as opposed to one law or standard, offers your organization the ability to comply with multiple privacy requirements at once, easily and quickly adapt to new privacy requirements, and build a culture of privacy within the organization.

Several fundamental privacy principles to consider when building out your internal privacy framework are:

- [Notices describing the use and disclosure of data](#)
- [Informed consent and other legal basis for collecting personal data](#)
- [Permitted uses, retention, and disclosure of personal data](#)
- [The right to access, amend, delete, and restrict the use of personal data](#)
- [Authorized third-party disclosures](#)
- [Breach Notification](#)
- [Data Integrity and Quality](#)
- [Data privacy program governance](#)

Depending on the nature of your organization's processing activities and the type of personal data that you process, there may be specific considerations that you will have to take into account such as different types of data processing impact assessments, international data transfers, and specific data retention standards.



How a Privacy Audit Benefits Your Organization

You want your organization to be seen as an organization that respects data privacy, but compliance is not an option when it comes to privacy laws and regulations. Complying with privacy laws and regulations can help prevent losses and protect your organization and customer data. Not only is adhering to privacy laws and regulations required of you by law but it also shows your commitment to your clients and their sensitive information.

You can use data privacy as a strategic advantage to build and maintain client relations both domestically and internationally. By complying with privacy laws like GDPR, you'll open your organization up to doing business with clients conducting business in the EU. Ongoing privacy compliance can also allow you to stand out amongst other competitors in your field and develop new products and services that can be trusted with personal data.

Alternatively, you could lose clients, face legal ramifications, and negatively affect your organization's reputation if you suffer a preventable data breach or regulatory violation. The consequences for violating data privacy laws could include hefty legal fines, ongoing by regulatory authorities, civil litigation by data subjects, and even shutting down your business.

Don't leave your reputation, clients, or your organization's success to chance. Pursue a privacy audit so that your organization is compliant with the various privacy laws that apply to your organization, and so you can have peace of mind about your business practices and client data.

How the Privacy Audit Process Works

Your path to privacy compliance will follow these 6 steps. At KirkpatrickPrice, our privacy auditors will guide you through each step so you can be confident that your privacy journey will end in success.

1 Scoping and Planning

There are many privacy laws and regulations in place both within the US and internationally, and knowing which laws apply to your organization can be confusing without a privacy professional helping you navigate the space. Our privacy auditors will work with you to see what types of data you're collecting, how you're collecting it, and how you're retaining that data as well as identifying where your clients are, all to determine which privacy laws and regulations your organization is expected to uphold.

2 Gap Assessment

We recommend that you undergo a privacy gap assessment before the actual privacy audit. A gap assessment will quickly clarify how your organization's privacy practices compare to the required regulations and privacy principles.

During the gap assessment, a privacy auditor will spend time with your organization to understand how you use, disclose, and retain personal data during business operations. Your auditor will clearly identify any operational, reporting, and compliance gaps before offering remediation strategies that are tailored to your business and compliance needs.

3 Remediation Plan

After your gap assessment, your privacy auditor will provide you with a remediation plan with resources to help fix any gaps that were identified in your organization's use, disclosure, or retention of personal data within your organization. By following the remediation plan, you're setting your organization up for a smoother audit down the road and the capability to implement new business and new privacy requirements with confidence and expertise.

4 Advisory Services

Our privacy auditors will then provide advisory services for you during your remediation efforts. Advisory services can help you implement your remediation plan by increasing your capacity, expertise, and accountability, allowing you to strengthen your organization's privacy posture and achieve your compliance goals.

5 The Audit

Once you have addressed your compliance gaps, you can begin your audit by uploading policies and evidence and connecting to your auditor through our proprietary audit application, the [Online Audit Manager](#). Your auditor will review your documentation and confirm whether all requirements are included within your policies and procedures.

Where the gap analysis is an in-depth discussion, the audit requires additional validation and evidence sampling so an important part of the audit is the onsite visit where the auditor can see your operations in action, interview key personnel, and observe your data privacy processes. Our direct analysis of your people, processes, and technology ensures that all aspects of your organization meet the requirements of the privacy laws that apply to you by interviewing personnel and observing processes.

At KirkpatrickPrice, we conduct a variety of privacy audits, including dedicated SOC 2 Privacy engagements, GDPR, CCPA/CPRA, HIPAA, FISMA, NIST, Microsoft SSPA, and more. Privacy touches every part of an organization, so we make sure you're complying with any relevant privacy law or regulation. If you need assurance about your compliance with multiple privacy frameworks, our expertise, tools, and processes allow us to audit multiple privacy frameworks simultaneously.

6 Report Delivery

When your organization completes a privacy audit, you receive a report stating the auditor's opinion on the effectiveness of your controls regarding the processing and protection of personal data. We will also ensure you understand the purpose behind each privacy requirement. By the end of your privacy audit, you can show off your report knowing that you received a quality audit from an experienced firm.

Major Data Privacy Laws and Regulations

Data privacy laws and regulations are being created and enforced all over the world. It's important to stay up to date on the latest laws that apply to your organization to make sure you're remaining compliant. We've compiled a list of some of the most common data privacy laws below.

US Data Privacy Laws:

[Federal Trade Commission Act \(FTC Act\)](#)

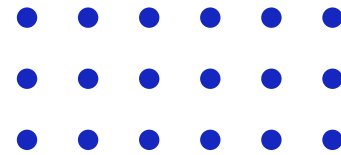
The FTC Act holds organizations accountable for how they handle individual's data. This act is designed to prevent unfair methods of competition and deceptive acts or practices in the marketplace. The two main goals of the FTC Act were to make sure competition between businesses was fair and to protect customers against fraudulent business practices.

[The Gramm-Leach-Bliley Act \(GLBA\)](#)

The GLBA is a regulation enforced by the FTC stating that all financial institutions disclose how they handle and share customer data. This law requires that these institutions have a policy in place to protect consumer data from security threats.

[Fair Credit Reporting Act \(FCRA\)](#)

The FCRA revolves around the protection of personal data that's collected by consumer reporting agencies such as credit bureaus, medical information companies, and tenant screening services.



[Health Insurance Portability and Accountability Act \(HIPAA\)](#)

HIPAA protects your personal health information (PHI) from being shared without your consent. The act protects patient-doctor confidentiality and prevents patient data from being shared with collaborators. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) enforces compliance with the HIPAA Privacy, Security, and Breach Notification Rules.

The HIPAA Privacy Rule is a national standard intended to protect patient's (PHI). The Privacy Rule requires healthcare organizations and their third parties to implement appropriate safeguards to protect the privacy of this information. It regulates things like appropriate use and disclosure of PHI, patient access to PHI, and patient rights.

[Family Educational Rights and Privacy Act \(FERPA\)](#)

FERPA is one of the most significant federal regulations in the education sector, aimed at protecting the privacy of students and their parents. The act governs the access and privacy of educational information and records, such as enrollment information, GPAs, billing information, student course schedules, and student financial records.

[Children's Online Protection Act \(COPPA\)](#)

COPPA places rules and regulations on what organizations can do with the data of children under the age of 13. One of the requirements set into place by this act includes a privacy policy that details data practices.

Many of the US states have passed data privacy laws in the past few years to protect the data of their residents. Many of these acts were based off Europe's GDPR. Although the acts listed below are the only ones who have official legislation in place, many other states have similar policies in the works. Even if your organization is not based in one of these states, you are required to adhere to these data privacy laws and regulations if you do business with any clients who do live in these states.

- [California Consumer Privacy Act \(CCPA\)](#)
- [Virginia Consumer Data Protection Act \(CDPA\)](#)
- [Colorado Privacy Act \(ColoPA\)](#)
- [Utah Consumer Privacy Act \(UCPA\)](#)
- [Connecticut Data Privacy Act \(CTDPA\)](#)

International Data Privacy Laws:

[General Data Protection Regulation \(GDPR\)](#)

In 2016, GDPR was introduced in Europe and is one of the toughest data privacy and security acts that currently exists. Even if an organization is not based in Europe, GDPR applies to any organization that does business with European citizens.

[The United Kingdom General Data Protection Regulation \(UK GDPR\)](#)

In 2018, the UK created the Data Protection Act 2018, which is the UK's implementation of GDPR.

[The Personal Information Protection and Electronic Documents Act \(PIPEDA\)](#)

PIPEDA is a Canadian privacy law that applies to private-sector organizations that collect, use, or disclose personal information in the course of a commercial activity, including the selling, bartering or leasing of donor, membership or other fundraising lists.

[Brazilian General Data Protection Law \(LGPD\)](#)

The LGPD aims to unify different Brazilian laws that regulate the processing of personal data. Like Europe's GDPR, the LGPD applies to the processing of data by organizations within Brazil in addition to organizations outside Brazil under certain circumstances.

[The Personal Information Protection Law \(PIPL\)](#)

The PIPL is China's first comprehensive law regarding personal information and data privacy.



Partner with KirkpatrickPrice to Meet All of Your Privacy Compliance Goals

Going through a privacy engagement can be confusing and challenging, but when you partner with KirkpatrickPrice, it doesn't have to be. We've been in your shoes and know how difficult it can be to keep up with all of the privacy laws and regulations that apply to your organization. When you work with KirkpatrickPrice, you'll be partnering with dedicated privacy experts.

You can stop feeling like you're missing something and stop being surprised when a client or attacker finds something that wasn't in your report. You can stop feeling worried that you're wasting time using someone who isn't advanced enough to thoroughly test your environment. Instead, you'll have a report that gets you ready for your next steps, allows you to say yes to client requests, opens up new and exciting business opportunities, and brings you the assurance you deserve. Privacy will no longer be a mystery.

To get started on your privacy audit, call one of our experts today at 800-779-2701 or visit www.kirkpatrickprice.com.

P.S. – Let's stay connected! Follow KirkpatrickPrice on LinkedIn, subscribe to our YouTube channel, or sign up for our monthly newsletter, The Readiness Report.

